ISM MP, Mathématiques
Année 2024/2025

Feuille d'exercices n°15

Exercice 1 (***)

On pose $$\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b, (a,b) \in \mathbb{Z}^2\}$$

1. Soient u, v dans $\mathbb{Z}[\mathrm{i}]$ avec $v \neq 0$. Montrer qu'il existe un couple $(q,r) \in \mathbb{Z}[\mathrm{i}]^2$ tel que $u = qv + r$ et $|r| < |v|$.
2. Montrer que les idéaux de $(\mathbb{Z}[\mathrm{i}], +, \times)$ sont exactement les $v\mathbb{Z}[\mathrm{i}]$ avec $v \in \mathbb{Z}[\mathrm{i}]$.

Corrigé : 1. Notons $\dfrac{u}{v} = x + \mathrm{i}y$ avec x et y réels et posons a et b les plus proches entiers relatifs respectivement de x et y. On a

$$|a - x| \leqslant \frac{1}{2} \quad \text{et} \quad |b - y| \leqslant \frac{1}{2}$$

Notant $q = a + \mathrm{i}b$, il vient $$\left|\frac{u}{v} - q\right| = \sqrt{(x-a)^2 + (y-b)^2} \leqslant \frac{1}{2}$$

Posant $v = u - qv$, on a q, r dans $\mathbb{Z}[\mathrm{i}]$ et $|r| \leqslant \dfrac{1}{2}|v| < |v|$. On conclut

$$\boxed{\text{Il existe un couple } (q,r) \in \mathbb{Z}[\mathrm{i}]^2 \text{ tel que } u = qv + r \text{ et } |r| < |v|.}$$

2. Pour $v \in \mathbb{Z}[\mathrm{i}]$, on sait que $v\mathbb{Z}[\mathrm{i}]$ est un idéal de $\mathbb{Z}[\mathrm{i}]$. Montrons que ce sont les seuls idéaux possibles. Soit I idéal de $\mathbb{Z}[\mathrm{i}]$ non nul. On note v un élément de I de module minimal. Par absorption, on a $v\mathbb{Z}[\mathrm{i}] \subset \mathrm{I}$. Réciproquement, soit $u \in \mathrm{I}$. D'après le résultat de la question précédente, il existe $(q,r) \in \mathbb{Z}[\mathrm{i}]^2$ tel que $u - qv = r$ et $|r| < |v|$. Or, on a $u - qv \in \mathrm{I}$ d'où $r = 0$ par minimalité de $|v|$. Ainsi, on a $u \in v\mathbb{Z}[\mathrm{i}]$ et on conclut

$$\boxed{\text{Les idéaux de } \mathbb{Z}[\mathrm{i}] \text{ sont exactement les } v\mathbb{Z}[\mathrm{i}] \text{ avec } v \in \mathbb{Z}[\mathrm{i}].}$$

Exercice 2 (****)

Un anneau intègre est dit *principal* si tout idéal de A est engendré par un élément. On note $\mathrm{A} = \mathbb{Z}[\mathrm{i}\sqrt{5}] = \left\{a + \mathrm{i}b\sqrt{5},\ (a,b) \in \mathbb{Z}^2\right\}$ muni des opérations $(+, \times)$.

1. Vérifier que $(\mathrm{A}, +, \times)$ est un anneau commutatif.
2. Pour $z \in \mathrm{A}$, on note $\mathrm{N}(z) = z\bar{z}$. Vérifier que

$$\forall (z, z') \in \mathrm{A}^2 \qquad \mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$$

   En déduire $\mathrm{U}(\mathrm{A})$.
3. Après avoir vérifié que $(1 + \mathrm{i}\sqrt{5}) \times (1 - \mathrm{i}\sqrt{5}) = 2 \times 3$, conclure que A n'est pas principal.

Corrigé : 1. On a $1 = 1 + 0 \times \mathrm{i}\sqrt{5} \in \mathrm{A}$. Soient (a,b) et (c,d) dans $\mathbb{Z}^2$. On trouve

$$a + \mathrm{i}b\sqrt{5} - \left(c + \mathrm{i}d\sqrt{5}\right) = a - c + \mathrm{i}(b-d)\sqrt{5} \in \mathrm{A}$$

et $$\left(a + \mathrm{i}b\sqrt{5}\right)\left(c + \mathrm{i}d\sqrt{5}\right) = (ac - 5bd) + \mathrm{i}\,(ad + bc)\,\sqrt{5} \in \mathrm{A}$$

ce qui prouve que A est un sous-anneau de $(\mathbb{C}, +, \times)$ et par conséquent

$$\boxed{\text{L'ensemble } (\mathrm{A},+,\times) \text{ est un anneau commutatif.}}$$

2. Soit $(z,z')\in \mathrm{A}^2$. Par propriétés sur les complexes, il vient

$$\mathrm{N}(zz') = (zz')\left(\overline{zz'}\right) = zz'\bar{z}\bar{z'} = z\bar{z}z'\bar{z'}$$

D'où $$\boxed{\forall (z,z')\in \mathrm{A}^2 \qquad \mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')}$$

On a $$\forall (a,b)\in\mathbb{Z}^2 \qquad \mathrm{N}\left(a+\mathrm{i}b\sqrt{5}\right) = \left(a+\mathrm{i}b\sqrt{5}\right)\left(a-\mathrm{i}b\sqrt{5}\right) = a^2+5b^2 \in \mathbb{N}$$

Soit $(a,b)\in\mathbb{Z}^2$ tel que $a+\mathrm{i}b\sqrt{5}\in \mathrm{U}(\mathbb{Z}[\mathrm{i}\sqrt{5}])$. Il existe $(c,d)\in\mathbb{Z}^2$ tel que $(a+\mathrm{i}b\sqrt{5})(c+\mathrm{i}d\sqrt{5}) = 1$ et

$$\mathrm{N}\left((a+\mathrm{i}b\sqrt{5})(c+\mathrm{i}d\sqrt{5})\right) = \mathrm{N}(a+\mathrm{i}b\sqrt{5})\mathrm{N}(c+\mathrm{i}d\sqrt{5}) = \mathrm{N}(1) = 1$$

d'où $$(a,b)\in\{(1,0),(-1,0)\}$$

La réciproque est immédiate et on conclut

$$\boxed{\mathrm{U}(\mathbb{Z}[\mathrm{i}\sqrt{5}]) = \{(1,0),(-1,0)\}}$$

3. Sans difficulté, on constate l'égalité

$$(1+\mathrm{i}\sqrt{5})\times(1-\mathrm{i}\sqrt{5}) = 2\times 3$$

Un élément p de A est dit *irréductible* si $p\notin \mathrm{U}(\mathrm{A})$ et si

$$\forall (a,b)\in\mathrm{A}^2 \qquad p=ab \quad\Longrightarrow\quad a\in\mathrm{U}(\mathrm{A}) \quad \text{ou} \quad b\in\mathrm{U}(\mathrm{A})$$

C'est exactement la même notion que celle vue dans $\mathbb{K}[\mathrm{X}]$. Vérifions que $1+\mathrm{i}\sqrt{5}$ est irréductible. Supposons que $1+\mathrm{i}\sqrt{5} = uv$ avec $(u,v)\in\mathrm{A}^2$. Il vient

$$\mathrm{N}(1+\mathrm{i}\sqrt{5}) = 6 = \mathrm{N}(uv) = \mathrm{N}(u)\mathrm{N}(v) \quad\Longrightarrow\quad \mathrm{N}(u)\in\{1,2,3,6\}$$

On vérifie sans difficulté que $\mathrm{N}(u)\notin\{2,3\}$ ce qui impose u ou v dans $\mathrm{U}(\mathrm{A})$ et prouve donc que $1+\mathrm{i}\sqrt{5}$ est irréductible. De même, on établit que 2 et 3 sont irréductibles. Supposons A principal. Alors, il existe $x\in\mathrm{A}$ tel que $(x) = \left(1+\mathrm{i}\sqrt{5}\right)+(2)$ d'où $x|1+\mathrm{i}\sqrt{5}$ et $x|2$. On en déduit $x\in\mathrm{U}(\mathrm{A})$ et par conséquent

$$\left(1+\mathrm{i}\sqrt{5}\right)+(2) = \mathrm{A}$$

On dispose alors de $(u,v)\in\mathrm{A}^2$ tel que

$$\left(1+\mathrm{i}\sqrt{5}\right)u+2v = 1$$

puis $$\left(1+\mathrm{i}\sqrt{5}\right)3u+6v = \left(1+\mathrm{i}\sqrt{5}\right)\left(3v+\left(1-\mathrm{i}\sqrt{5}\right)v\right) = 3$$

d'où $1+\mathrm{i}\sqrt{5}|3$ ce qui est faux. On conclut

$$\boxed{\text{L'anneau A n'est pas principal.}}$$

Remarque : En fait, l'égalité $(1+\mathrm{i}\sqrt{5})\times(1-\mathrm{i}\sqrt{5}) = 2\times 3$ prouve que l'anneau A n'est pas *factoriel*, *i.e.* intègre et tel que tout élément non nul admet une décomposition en facteurs irréductibles, unique à l'ordre près. On peut démontrer qu'un anneau principal est factoriel.

Exercice 3 (***)

Soit $(\mathbb{K}, +, \times, \cdot)$ une $\mathbb{R}$-algèbre commutative, intègre, de dimension finie $n \geqslant 2$.

1. Soit a un élément non nul de $\mathbb{K}$. Pour $x \in \mathbb{K}$, on pose $f_a(x) = ax$. Montrer que f est un automorphisme linéaire de $\mathbb{K}$.
2. Soit $a \in \mathbb{K} \setminus \mathbb{R}$. Montrer que la famille $(1, a)$ est libre mais pas $(1, a, a^2)$.
3. Montrer que l'on peut trouver $\mathrm{i} \in \mathbb{K}$ tel que $\mathrm{i}^2 = -1$. En déduire que $\mathbb{K}$ est une $\mathbb{R}$-algèbre isomorphe à $\mathbb{C}$.

Corrigé : 1. On rappelle que $(\mathbb{K}, +, \cdot)$ est un $\mathbb{R}$-ev de dimension finie, $(\mathbb{K}, +, \times)$ est un anneau et qu'on a

$$\forall (\lambda, x, y) \in \mathbb{R} \times \mathbb{K}^2 \qquad (\lambda \cdot x)y = \lambda \cdot (xy) = x(\lambda \cdot y)$$

Ainsi

$$\forall (\lambda, x, y) \in \mathbb{R} \times \mathbb{K}^2 \qquad f_a(x + \lambda y) = a(x + \lambda \cdot y) = ax + \lambda \cdot (ay) = f_a(x) + \lambda \cdot f_a(y)$$

Puis, par intégrité de $\mathbb{K}$, il vient

$$\forall x \in \mathbb{K} \qquad f_a(x) = 0 \iff ax = 0 \iff x = 0$$

L'application f_a est donc un endomorphisme injectif dans un $\mathbb{R}$-ev de dimension finie et par conséquent

$$\boxed{\forall a \in \mathbb{K}^* \qquad f_a \in \mathrm{GL}(\mathbb{K})}$$

Remarque : On en déduit notamment que $\mathbb{K}$ est un corps puisque pour tout $a \in \mathbb{K}^*$, on dispose, par surjectivité de f_a, de $b \in \mathbb{K}$ tel que $f_a(b) = 1$, c'est-à-dire $ab = 1$.

2. Soit $a \in \mathbb{K} \setminus \mathbb{R}$. Ce choix est possible puisque $\mathbb{K}$ est un $\mathbb{R}$-ev de dimension $n \geqslant 2$. La famille $(1, a)$ n'est pas liée, sans quoi on aurait a colinéaire à 1 puisque 1 est non nul, ce qui impliquerait a réel. La famille $\left(a^k\right)_{k \in [\![0\,;n]\!]}$ est une famille de $n+1$ vecteurs dans $\mathbb{K}$ qui est un $\mathbb{R}$-ev de dimension n. Il s'agit donc d'une famille liée d'où l'existence de $(\alpha_k)_{k \in [\![0\,;n]\!]} \in \mathbb{R}^{n+1} \setminus \{0_{\mathbb{R}^{n+1}}\}$ tel que $\sum_{k=0}^{n} \alpha_k a^k = 0$. Ainsi, posant $\mathrm{R} = \sum_{k=0}^{n} \alpha_k \mathrm{X}^k$, on a montré

$$\boxed{\text{Il existe un polynôme non nul } \mathrm{R} \in \mathbb{R}[\mathrm{X}] \text{ tel que } \mathrm{R}(a) = 0.}$$

Considérant l'écriture de R comme produit de facteurs irréductibles dans $\mathbb{R}[\mathrm{X}]$, on en déduit, par intégrité de $\mathbb{K}$, qu'il existe $\mathrm{P}_a \in \mathbb{R}[\mathrm{X}]$ irréductible tel que $\mathrm{P}_a(a) = 0$. On a $\deg \mathrm{P}_a > 1$ par liberté de $(1, a)$ et comme les polynômes irréductibles de $\mathbb{R}[\mathrm{X}]$ sont de degré 1 ou 2, on conclut $\deg \mathrm{P}_a = 2$ d'où

$$\boxed{\text{La famille } (1, a) \text{ est libre mais pas } (1, a, a^2).}$$

3. On peut choisir P_a unitaire. On note $\mathrm{P}_a = \mathrm{X}^2 + \alpha \mathrm{X} + \beta$ avec α, β réels tels que $\alpha^2 - 4\beta < 0$. Puis, il vient

$$\begin{aligned} \mathrm{P}_a(a) = 0 \iff a^2 + \alpha a + \beta = 0 &\iff \left(a + \frac{\alpha}{2}\right)^2 + \frac{4\beta - \alpha^2}{4} = 0 \\ &\iff \left(\frac{2}{\sqrt{4\beta - \alpha^2}}\left(a + \frac{\alpha}{2}\right)\right)^2 + 1 = 0 \end{aligned}$$

On pose

$$b = \frac{2}{\sqrt{4\beta - \alpha^2}}\left(a + \frac{\alpha}{2}\right)$$

L'élément b vérifie alors $b^2+1=0$. La famille $(1,b)$ est libre sans quoi b serait réel et on note $\mathrm{A}=\mathrm{Vect}\,(1,b)$. Montrons $\mathrm{A}=\mathbb{K}$. On procède par l'absurde en considérant $c\in\mathbb{K}\setminus\mathrm{A}$. En particulier, on a $c\in\mathbb{K}\setminus\mathbb{R}$ et en procédant comme pour la construction de b, on obtient l'existence de $d\in\mathrm{Vect}\,(1,c)$ tel que $d^2+1=0$. Il s'ensuit $d^2=b^2$ puis $(d-b)(d+b)=0$ par commutativité de $\mathbb{K}$ et par intégrité $d=b$ ou $d=-b$. Il en résulte que $b=\pm d=\lambda+\mu c$ avec λ,μ réels et $\mu\neq 0$ sinon b réel d'où $c\in\mathrm{Vect}\,(1,b)=\mathrm{A}$ ce qui est faux. On en déduit que $\mathbb{K}=\mathrm{Vect}\,(1,b)$. Enfin, on considère

$$\varphi\colon\begin{cases}\mathbb{C}\longrightarrow\mathbb{K}\\ z\longmapsto \mathrm{Re}\;z+b\,\mathrm{Im}\;z\end{cases}$$

et on vérifie sans difficulté que φ est un isomorphisme d'algèbres. On conclut

$$\boxed{\text{La }\mathbb{R}\text{-algèbre }\mathbb{K}\text{ est isomorphe à }\mathbb{C}.}$$

Exercice 4 (***)

Déterminer dans $\mathbb{K}[\mathrm{X}]$ les polynômes divisibles par leur polynôme dérivé.

Corrigé : Soit $\mathrm{P}\in\mathbb{K}[\mathrm{X}]$. Si P' divise P, alors comme $\deg\mathrm{P}=1+\deg\mathrm{P}'$, on a $\mathrm{P}=\lambda(\mathrm{X}-\alpha)\mathrm{P}'$. Donc P admet une racine α. Soit m son ordre et notons $\mathrm{P}=\lambda(\mathrm{X}-\alpha)^m\mathrm{Q}$ avec $\mathrm{Q}(\alpha)\neq 0$. Ainsi $\mathrm{P}'=(\mathrm{X}-\alpha)^{m-1}\mathrm{Q}$. Mais par dérivation

$$\mathrm{P}'=\lambda(\mathrm{X}-\alpha)^{m-1}\left[m\mathrm{Q}+(\mathrm{X}-\alpha)\mathrm{Q}'\right]$$

d'où

$$\mathrm{Q}=\lambda\left[m\mathrm{Q}+(\mathrm{X}-\alpha)\mathrm{Q}'\right]$$

En évaluant pour $\mathrm{X}=\alpha$, on trouve $\lambda m=1$ puis

$$(\mathrm{X}-\alpha)\mathrm{Q}'=0\Longrightarrow\mathrm{Q}'=0$$

On conclut $\boxed{\text{Si P}'\text{divise P, alors P de la forme }\lambda(\mathrm{X}-\alpha)^m\text{ avec }\alpha\in\mathbb{K}\text{ et }m\text{ entier.}}$

Variantes : 1. Dans l'ensemble des fractions rationnelles $\mathbb{C}(\mathrm{X})$, on sait que $\dfrac{\mathrm{P}'}{\mathrm{P}}=\displaystyle\sum_{i=1}^{r}\frac{m_i}{\mathrm{X}-\alpha_i}$ avec α_i les racines et m_i leurs multiplicités. Or, on a P' divise P d'où $\mathrm{P}=\lambda(\mathrm{X}-\alpha)\mathrm{P}'$ d'où $\dfrac{\mathrm{P}'}{\mathrm{P}}=\dfrac{1}{\lambda(\mathrm{X}-\alpha)}$ et on en déduit $r=1$. On retrouve le résultat précédent.
2. Si $\mathbb{K}=\mathbb{R}$, on peut aussi montrer, par l'absurde, qu'un polynôme P solution possède une unique racine. En effet, sinon, on pourrait, avec le théorème de Rolle, trouver un racine de P' entre deux racines consécutives de P qui serait alors racine de P, ce qui est absurde.

Exercice 5 (****)

Pour P dans $\mathbb{C}[\mathrm{X}]$, on note $\mathrm{Z}(\mathrm{P})$ l'ensemble des racines de P.

1. Soit P dans $\mathbb{C}[\mathrm{X}]$ avec $\deg\mathrm{P}\geqslant 1$. Montrer

$$\mathrm{Card}\;\mathrm{Z}(\mathrm{P})=\deg\mathrm{P}-\deg(\mathrm{P}\wedge\mathrm{P}')$$

2. Soient P,Q des polynômes non constants de $\mathbb{C}[\mathrm{X}]$ tels que $\mathrm{Z}(\mathrm{P})=\mathrm{Z}(\mathrm{Q})$ et $\mathrm{Z}(\mathrm{P}-1)=\mathrm{Z}(\mathrm{Q}-1)$. Montrer que $\mathrm{P}=\mathrm{Q}$.

Corrigé : 1. Notons $\mathrm{P} = \lambda \prod_{i=1}^{r} (\mathrm{X} - \alpha_i)^{m_i}$ avec λ, α_i des complexes et m_i des entiers non nuls. Comme α_i racine de P' de multiplicité $m_i - 1$, on a

$$\mathrm{P} \wedge \mathrm{P}' = \prod_{i=1}^{r} (\mathrm{X} - \alpha_i)^{m_i - 1}$$

et
$$\deg(\mathrm{P} \wedge \mathrm{P}') = \sum_{i=1}^{r} (m_i - 1) = \deg \mathrm{P} - r$$

Ainsi
$$\boxed{\text{Card } \mathrm{Z}(\mathrm{P}) = \deg \mathrm{P} - \deg(\mathrm{P} \wedge \mathrm{P}')}$$

2. Notons $n = \deg \mathrm{P}$ et $m = \deg \mathrm{Q}$. On suppose $n \geqslant m$. Posons $\mathrm{R} = \mathrm{P} - \mathrm{Q}$. On a $\mathrm{Z}(\mathrm{R}) \supset \mathrm{Z}(\mathrm{P}) \cup \mathrm{Z}(\mathrm{P} - 1)$ et $\mathrm{Z}(\mathrm{P}) \cap \mathrm{Z}(\mathrm{P} - 1) = \varnothing$ d'où

$$\text{Card } \mathrm{Z}(\mathrm{R}) \geqslant \text{Card } \mathrm{Z}(\mathrm{P}) + \text{Card } \mathrm{Z}(\mathrm{P} - 1)$$

D'après le résultat de la question précédente, on a

$$\text{Card } \mathrm{Z}(\mathrm{P}) = n - \deg(\mathrm{P} \wedge \mathrm{P}') \quad \text{et} \quad \text{Card } \mathrm{Z}(\mathrm{P} - 1) = n - \deg((\mathrm{P} - 1) \wedge \mathrm{P}')$$

Les polynômes P et $\mathrm{P} - 1$ sont premiers entre eux car sans racine commune et par conséquent, on a $\mathrm{P} \wedge \mathrm{P}'$ et $(\mathrm{P} - 1) \wedge \mathrm{P}'$ diviseurs de P' qui sont premiers entre eux d'où $(\mathrm{P} \wedge \mathrm{P}')((\mathrm{P} - 1) \wedge \mathrm{P}') | \mathrm{P}'$ et par conséquent

$$\deg(\mathrm{P} \wedge \mathrm{P}') + \deg((\mathrm{P} - 1) \wedge \mathrm{P}') \leqslant \deg \mathrm{P}' = n - 1$$

Il s'ensuit
$$\text{Card } \mathrm{Z}(\mathrm{R}) \geqslant 2n - (n - 1) = n + 1 \quad \text{et} \quad \deg \mathrm{R} \leqslant n$$

On en déduit $\mathrm{R} = 0$ et par conséquent

$$\boxed{\mathrm{P} = \mathrm{Q}}$$

Exercice 6 (***)

Soient P, Q deux polynômes de $\mathbb{C}[\mathrm{X}]$ non constants avec $\deg \mathrm{P} = n$ et $\deg \mathrm{Q} = m$. On pose

$$\Phi : \begin{cases} \mathbb{C}_{m-1}[\mathrm{X}] \times \mathbb{C}_{n-1}[\mathrm{X}] & \longrightarrow \mathbb{C}_{n+m-1}[\mathrm{X}] \\ (\mathrm{U}, \mathrm{V}) & \longmapsto \mathrm{UP} + \mathrm{VQ} \end{cases}$$

1. Montrer que Φ est bien définie, linéaire puis déterminer sa matrice dans les bases canoniques des espaces de départ et d'arrivée. On notera $\mathrm{Res}[\mathrm{P}, \mathrm{Q}]$ le déterminant de cette matrice appelé *résultant* de P et Q.

2. Établir
$$\Phi \text{ bijective} \iff \mathrm{P} \wedge \mathrm{Q} = 1$$

3. Soit $\mathrm{P} = \mathrm{X}^3 + px + q$ avec $p, q \in \mathbb{C}$. Montrer que P admet une racine double si et seulement si $4p^3 + 27q^2 = 0$.

Corrigé : 1. Soit $(\mathrm{U}, \mathrm{V}) \in \mathbb{C}_{m-1}[\mathrm{X}] \times \mathbb{C}_{n-1}[\mathrm{X}]$. On a $\deg \mathrm{UP} \leqslant n + m - 1$ et $\deg \mathrm{VQ} \leqslant n + m - 1$ d'où $\deg \mathrm{UP} + \mathrm{VQ} \leqslant n + m - 1$. Par ailleurs, l'application Φ est linéaire par linéarité de la somme et du produit d'où

$$\boxed{\Phi \in \mathscr{L}(\mathbb{C}_{m-1}[\mathrm{X}] \times \mathbb{C}_{n-1}[\mathrm{X}], \mathbb{C}_{n+m-1}[\mathrm{X}])}$$

Supposons Φ bijective. En particulier, on a Φ surjective d'où

$$\exists (\mathrm{U}, \mathrm{V}) \in \mathbb{C}_{m-1}[\mathrm{X}] \times \mathbb{C}_{n-1}[\mathrm{X}] \quad | \quad \Phi(\mathrm{U}, \mathrm{V}) = \mathrm{UP} + \mathrm{VQ} = 1$$

La base canonique de $\mathbb{C}_{m-1}[X]\times\mathbb{C}_{n-1}[X]$ est constituée de $(X^i,0)_{0\leqslant i\leqslant m-1}$ suivi de $(0,X^{i-m})_{m\leqslant i\leqslant n+m-1}$. On trouve

$$\begin{pmatrix} a_0 & 0 & \dots & 0 & b_0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ a_n & & & a_0 & b_m & & & b_0 \\ 0 & \ddots & & \vdots & 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & a_n & 0 & \dots & 0 & b_m \end{pmatrix}$$

Sur ce schéma, on a supposé $n=m$ pour des raisons pratiques mais la forme obtenue a lieu pour tout couple d'entiers non nuls (n,m).

2. Supposons Φ bijective. D'après le théorème de Bezout, on en déduit $P\wedge Q=1$. Supposons $P\wedge Q=1$. On a

$$\Phi(U,V)=0 \iff UP=-VQ$$

D'après le lemme de Gauss, on en déduit $P|V$ et $Q|U$ mais $\deg V<\deg P$ et $\deg U<\deg P$ d'où $(U,V)=(0,0)$. Ainsi, l'application Φ est injective et comme on a

$$\dim \mathbb{C}_{m-1}[X]\times\mathbb{C}_{n-1}[X]=\dim\mathbb{C}_{m-1}[X]+\dim\mathbb{C}_{n-1}[X]$$

l'injectivité de Φ équivaut à sa bijectivité. Ainsi

$$\boxed{\Phi \text{ bijective} \iff P\wedge Q=1}$$

3. On considère Φ associée à P et P′. On a

$$P \text{ admet un racine double} \iff P\wedge P'\neq 1 \iff \det\Phi=0$$

On trouve
$$\det\Phi=\begin{vmatrix} q & 0 & p & 0 & 0 \\ p & q & 0 & p & 0 \\ 0 & p & 3 & 0 & p \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = q\begin{vmatrix} q & 0 & p & 0 \\ p & 3 & 0 & p \\ 0 & 0 & 3 & 0 \\ 1 & 0 & 0 & 3 \end{vmatrix} + p\begin{vmatrix} p & q & p & 0 \\ 0 & p & 0 & p \\ 1 & 0 & 3 & 0 \\ 0 & 1 & 0 & 3 \end{vmatrix}$$

En développant le premier déterminant sur la 3-ième ligne et le deuxième déterminant sur la première colonne, on trouve

$$\det\Phi=4p^3+27q^2$$

Ainsi
$$\boxed{P \text{ admet une racine double} \iff 4^3+27q^2=0}$$